



DE OLHO NO LANCE

Dicas de Segurança da
Informação para Empresas

ENTENDA O REAL VALOR DOS DADOS DO SEU NEGÓCIO

HOJE EM DIA, OS DADOS SÃO O BEM MAIS PRECioso DE UM NEGÓCIO!

Pois é, para qualquer empresa, os dados estão no topo da lista dos recursos valiosos, e são eles que fazem a empresa crescer e acontecer! Por isso, nós precisamos fazer de tudo para proteger esses dados, e assim, proteger a própria empresa e o negócio. Afinal, esses valiosos dados não podem cair em mão erradas, e nem serem usados de forma incorreta, perdidos e muito menos roubados, não é mesmo?



MAS QUE TAIS DADOS SÃO ESSES?

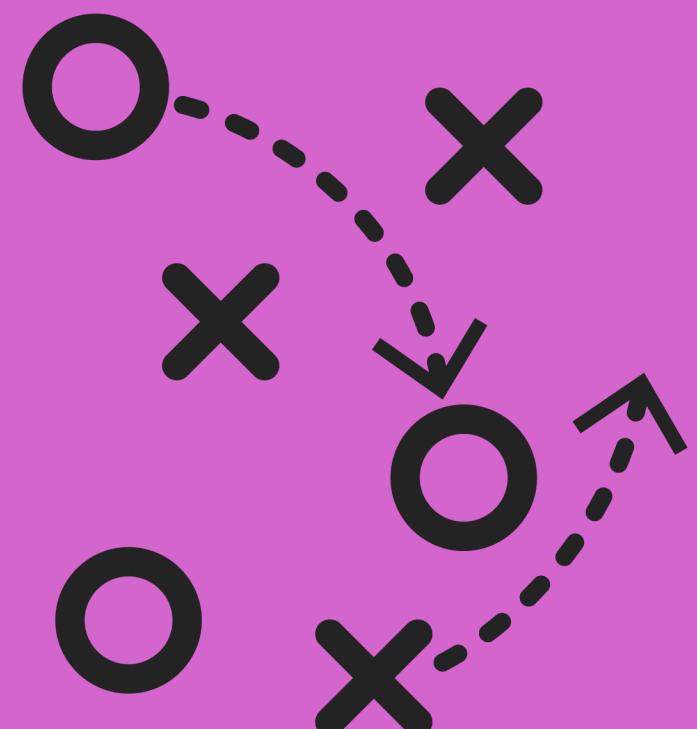
Quando falamos sobre dados, estamos falando de:

- Dados de clientes e funcionários (como CPF, nome, endereço, etc);
- Dados e informações administrativas da empresa (como o CNPJ e registros);
- Dados financeiros e bancários (como contas do banco, planilhas, cartões, etc);
- Contratos, notas fiscais, recibos, planilhas e documentos;
- Dados confidenciais, como estratégias de negócio e projetos.

E todos os tipos de dados que possam passar pelo seu negócio.

O QUE É DE VALOR PRECISA SER DEVIDAMENTE PROTEGIDO!

Seja gerando novos dados, tratando e usando os dados, guardando e até descartando esses dados após o uso, todos esses passos precisam ser feitos com muita segurança, protegendo os dados contra o uso incorreto, além de riscos, ameaças e criminosos.



OBEDECENDO A LEI E EVITANDO PREJUÍZO: É PRECISO PROTEGER OS DADOS

VOCÊ SABIA?



Atualmente, já existem leis, normas e regulamentos no mundo todo, que garantem o nosso direito à privacidade e também falam sobre a obrigação que as empresas têm de proteger os dados, tanto do próprio negócio e da empresa, quanto dos seus clientes também!

**É IMPORTANTE
OBEDECER A LEI E
TOMAR OS DEVIDOS
CUIDADOS**

Por isso, não importa qual o tamanho do seu negócio, é preciso prestar muita atenção em termos de contratos assinados com clientes e na sua responsabilidade de proteger os dados que você tem acesso.

Fica a dica: Ao lidar com clientes grandes, é muito comum assinar termos de responsabilidades, confidencialidade, de tratamento e proteção de dados. Por isso, fique de olho e leia os documentos com muito cuidado, obedecendo os contratos e as suas obrigações!

LEIS, NORMAS E REGULAMENTOS



No Brasil, a Lei Geral de Proteção de Dados (LGPD) cuida dos direitos dos titulares de dados pessoais - os donos dos dados, e regulamenta o que as empresas podem fazer e como devem cuidar dos dados. Existem também normas, como o conjunto da ISO 27000, que fala justamente sobre as recomendações de Segurança das Informações para serem seguidas pelas empresas e corporações.

Cuide da Proteção dos Dados desde o começo

Se você se preocupar com a segurança e a proteção dos seus dados desde o começo do seu negócio e no começo de cada projeto, tudo fica muito mais fácil! Afinal, quando você precisar provar que está cuidando bem dos dados, ou até mesmo sofrer um ataque, a sua segurança já vai estar a postos e preparada!

Um diferencial competitivo

Além disso, tomar os devidos cuidados e proteger os dados não só pode livrar o negócio de problemas com a Lei, mas também é o que o mercado chama de "diferencial competitivo", mostrando que você tem uma preocupação genuína e é transparente com o cliente, criando confiança e credibilidade.



Evite prejuízos e danos irreparáveis

Cuidar da Segurança e da Proteção dos Dados pode evitar grandes problemas e dores de cabeça, como ser alvo de ataques, acabando em prejuízos enormes e irreparáveis, congelando os negócios ou até colocando a própria existência da empresa em risco. É também uma forma de prevenir a perda de clientes, de funcionários ou até mesmo problemas perante a Lei. Viu só como é importante proteger os dados?

A SEGURANÇA DA INFORMAÇÃO E A PROTEÇÃO DE DADOS

É aqui que a Segurança da Informação entra em cena!

Tudo que a gente faz hoje em dia, fazemos pela internet e por meios digitais, não é mesmo? E isso não é diferente para as empresas e negócios! Seja usando websites e plataformas, aplicativos, redes sociais e tantas outras ferramentas online, quando você conecta o seu negócio com a internet, está expondo todos os dados que passam por essas plataformas e serviços à possíveis perigos, e por isso, você precisa saber se proteger.

Quem é que cuida da Segurança?

Muito prazer! A Segurança da Informação é a área que cuida da proteção dos dados, informações e sistemas digitais, defendendo esses dados contra ataques, criminosos, vazamentos, roubo de informações e fraudes. É uma área conhecida por ser técnica, mas calma lá! Isso não significa que a Segurança da Informação só pode ser feita por quem entende de computação, viu?



Proteger os Dados é uma responsabilidade de todos!

Pois é, a Segurança da Informação e a proteção de dados é uma responsabilidade de todo mundo que têm acesso aos dados e sistemas, mesmo que elas não sejam pessoas técnicas ou especialistas. Hoje em dia, já é uma área muito mais acessível, com recomendações e ferramentas que podem ser usadas e praticadas por todo mundo, não importa o nível de conhecimento!

Siga as recomendações e boas práticas

Micro e pequenas empresas não costumam ter áreas dedicadas para a Tecnologia e a Segurança das Informações, mas isso não é um problema. Ainda assim, é possível seguir e obedecer as recomendações de segurança, usar ferramentas e aplicativos seguros e adquirir práticas de prevenção contra riscos e ataques aos dados. A Segurança é pra todo mundo!

NÃO SEJA UM ALVO FÁCIL: A LEI DO MENOR ESFORÇO

Opa, será que você está na mira?

Ao contrário do que as pessoas pensam, lutar contra os criminosos da internet, golpistas e contra ameaças aos dados não é uma tarefa tão injusta - e nem tão difícil assim! Por isso, não perca as esperanças... Muitos criminosos e ataques agem por um princípio chamado de "Lei do Menor Esforço". Ou seja, eles querem o maior lucro, em menor tempo, com o menor risco e menor esforço. O que eles querem são alvos fáceis.



Se proteger é mais fácil do que parece!

Se os dados do seu negócio estiverem bem protegidos pelas práticas de segurança básicas e por ferramentas confiáveis (mesmo as que são facinhas de usar), sua empresa já estará protegida contra a grande maioria dos riscos e ameaças. Ufa!

Você não precisa ser um especialista para se conseguir se defender

Sendo assim, a sua empresa não precisa necessariamente de um time técnico ou de especialistas para cuidar da segurança. Tudo o que você precisa é de atenção às recomendações de segurança, praticando os hábitos seguros e tendo dedicação para proteger seus dados. O segredo é deixar de ser um alvo fácil, obedecendo o nosso passo a passo da Segurança.

PASSO 1: CUIDADO COM OS ATAQUES DE ENGENHARIA SOCIAL

Você sabe o que é Engenharia Social?

São táticas usadas pelos criminosos para te convencer a cometer erros e cair em golpes. Eles usam técnicas de manipulação para enganar as vítimas, mexendo com as emoções das pessoas e os sentidos. É triste, mas os criminosos se aproveitam de pessoas desatentas, ingênuas ou que não sabem se proteger contra os ataques.

Como os criminosos manipulam as vítimas
Assim, eles gostam de criar situações mentirosas, que parecem urgentes, ou inventam benefícios "super imperdíveis", para fazer a vítima agir por impulso. Eles podem se passar por pessoas, clientes e empresas conhecidas, podem enviar documentos falsos, links e arquivos infectados, pedir códigos de segurança ou até tentar convencer a vítima a fazer transações bancárias! Esses criminosos são cheios de criatividade.



OS TIPOS MAIS POPULARES DE ATAQUES:



Baiting (Isca): Os criminosos criam uma "isca" para chamar a atenção da vítima, como uma promoção, um benefício, uma oportunidade imperdível, boa demais para ser verdade. Geralmente o ataque vem acompanhado de um arquivo infectado para ser baixado, um link malicioso para clicar ou até um formulário para roubar os dados.

PEQUENO EXEMPLO:

Se você já ganhou algum sorteio especial que você nunca se inscreveu, ou te falaram que você ganhou um produto de graça, sem nunca ter pedido, então já tentaram te passar a perna!

Phishing (Pescaria): Pode ser um email falso, uma ligação ou até mesmo uma mensagem sms, por aplicativo ou inbox. O criminoso pode usar uma "isca" para enganar e "pescar" a vítima, convencendo ela a cometer um erro ou passar seus dados, sem nem perceber ou desconfiar do golpe.

PEQUENO EXEMPLO:

Será que você já recebeu um email de promoção com um botão bem brilhante pra você clicar? Ou até uma mensagem pelo celular, com um prêmio e um link bem estranho? Então você já recebeu um phishing!

Roubo de dados: O criminoso cria uma página falsa para enganar a vítima, convencendo ela a preencher os dados, seja usuário, senha, dados pessoais ou até bancários. Ele também pode fazer isso por ligação e até usando aplicativos que parecem inofensivos, ou que imitam um serviço já conhecido.

PEQUENO EXEMPLO:

O golpista envia uma mensagem dizendo que uma compra suspeita foi feita no seu nome, e te manda um link para uma página de login que parece a do banco, mas não é!

Roubo de acessos: Seja por mensagem, por email ou ligação, o golpista se passa por alguém de confiança e tenta convencer a vítima a passar o acesso das contas, clicando em uma permissão ou passando a senha e até um código de segurança.

PEQUENO EXEMPLO:

Os criminosos entram em contato por mensagem dizendo ser do suporte do banco ou de um serviço que você usa, inventando um problema e dizendo que precisam do seu código de segurança. Não caia nessa!

Personificação: O golpista finge ser uma pessoa de confiança ou uma empresa ou serviço conhecidos, copiando o logo e as cores, usando gravações de voz, um perfil ou conta falsa, fotos e dados roubados para passar mais credibilidade e convencer a vítima desatenta.



PEQUENO EXEMPLO:

Copiando a foto de uma pessoa da sua família ou um amigo, o golpista cria um perfil falso e entra em contato por mensagem, pedindo dinheiro ou ajuda financeira, inventando uma desculpa.

PASSO 2: CRIE HÁBITOS SEGUROS E SIGA AS BOAS PRÁTICAS DE SEGURANÇA



Eduque-se: Acompanhe as notícias e profissionais da área

Infelizmente é muito comum vermos notícias de golpes pela mídia, não é? Mas use isso a seu favor! Aproveite toda oportunidade para se informar e se educar, entendendo como esses golpes acontecem e consumindo conteúdo que ensina a se proteger e defender seus dados.

OLHA A DICA:

Você também pode usar as redes sociais para encontrar profissionais da área de privacidade e proteção de dados, Segurança da Informação e de conscientização em Segurança, para acompanhar as dicas e alertas contra as ameaças do momento.

Desconfie sempre

A maioria dos ataques cibernéticos e roubos de dados acontece pela interação entre pessoas, e não pelos sistemas. Os criminosos se aproveitam de pessoas distraídas e ingênuas, conseguindo os acessos e dados que precisam para causar prejuízo, sem muito esforço.

OLHA A DICA:

Sempre desconfie de situações inesperadas ou de pessoas desconhecidas, criando o hábito de prestar atenção e se proteger, mesmo que pareça uma situação inofensiva. É exatamente esse o disfarce dos criminosos.

Atenção redobrada com documentos e arquivos

Não saia clicando em links desconhecidos, nem baixe arquivos sem antes confirmar que o remetente é verdadeiro e confiável, ou que a situação é verídica. Os criminosos usam esses links e arquivos para infectar os seus dispositivos, sem que você perceba, ganhando acessos e roubando informações.

OLHA A DICA:

Você pode usar um desencurtador de URL antes de clicar em um link encurtado, ou acessar o site do VirusTotal.com para ver se o link é mesmo confiável.

Fique de olho nos detalhes

Ao receber um email, preste atenção no remetente, e confira se é confiável ou oficial. Além disso, procure por erros de ortografia, imagens desalinhadas ou elementos estranhos. Se for o caso, faça várias perguntas para confirmar a situação.

OLHA A DICA:

Se receber um link, você pode passar o mouse em cima, sem clicar, para ver o endereço que ele vai te levar. E, no navegador, preste muita atenção na URL (endereço do site), para saber se é o oficial.

Pesquise a veracidade da situação e cheque as fontes oficiais

Na dúvida, sempre cheque as fontes originais antes de qualquer coisa! Vá até o site oficial, tente contato com a pessoa da sua confiança pelos telefones e redes que você já conhece, use os aplicativos oficiais e pontos de consulta realmente confiáveis.

OLHA A DICA:

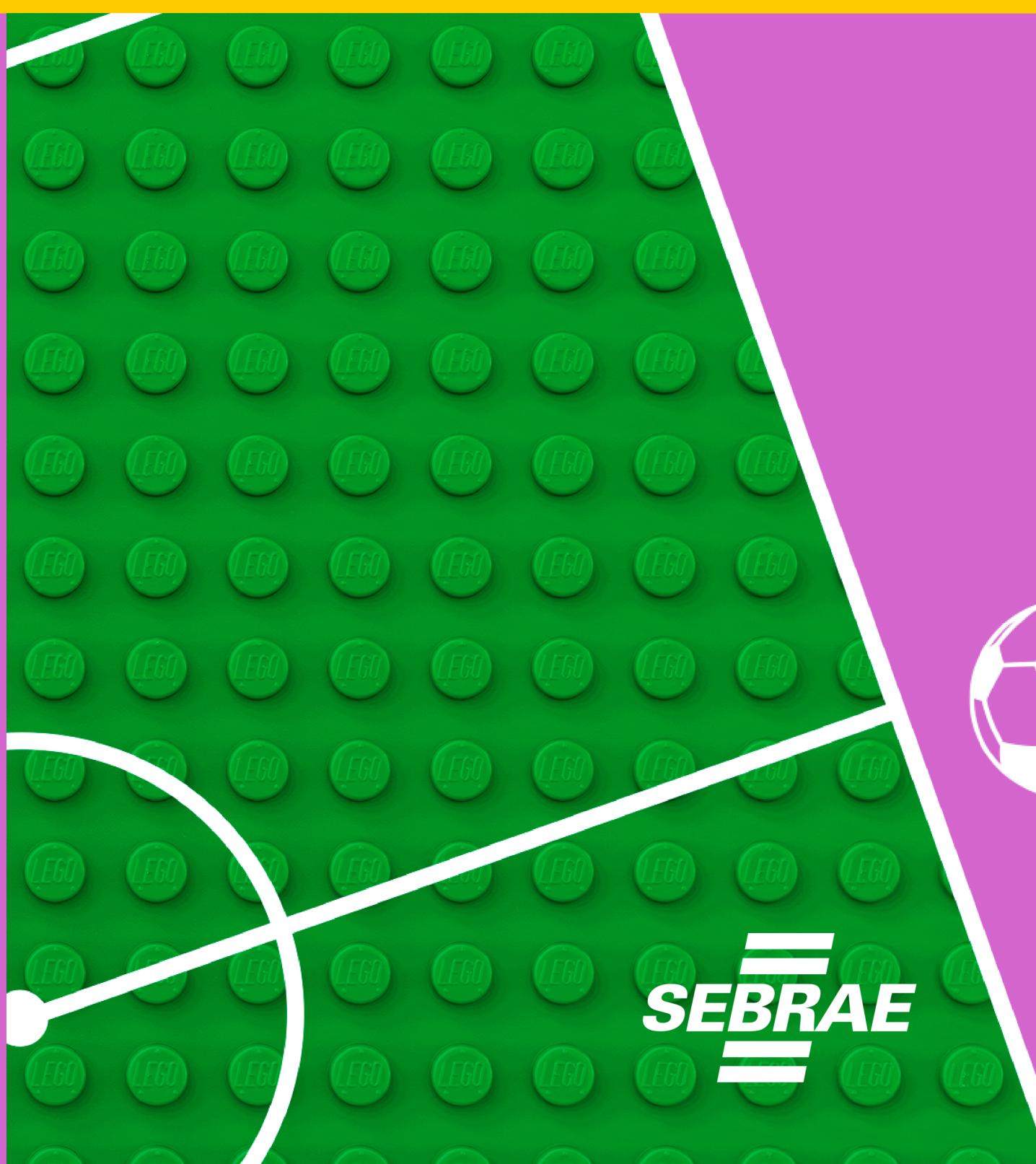
Uma busca rápida no próprio google ou no site oficial podem te salvar de enrascadas! Muita gente reclama de forma pública e denuncia golpes na internet.

Reporte os ataques para os serviços e de forma pública

Se você desconfiar que está em perigo ou sofrer um golpe, não interaja com o criminoso! Reporte como spam ou phishing, bloquee o canal de contato e denuncie a tentativa para os serviços afetados, seja por email ou até alertando de forma pública, por fóruns ou redes sociais.

OLHA A DICA:

Se você alertar os outros, você ajuda a parar o ataque não só para você, mas para muitas outras pessoas! Mas cuidado, evite compartilhar o ataque com links e arquivos. Prefira compartilhar apenas o print-screen do golpe, para não dar mais alcance para o atacante.





Cuidados nas redes sociais

Muitos ataques hoje em dia acontecem pelas redes sociais, principalmente pelo inbox, usando contas falsas. Preste muita atenção e não acredite em tudo que recebe, desconfiando sempre. Além disso, cuidado para não expor dados importantes do negócio nas redes, revelando informações que os criminosos podem roubar ou usar contra a sua empresa.

OLHA A DICA:

Lembre-se que todo mundo tem acesso à rede social, inclusive os criminosos. Será que você precisa mesmo postar sobre tudo, sem prestar atenção nos dados que estão sendo expostos?

Saiba para quem pedir ajuda

Cair em um golpe, ser vítima de um ataque ou cometer erros não são motivos para vergonha! Acredite, acontece com todo mundo. Quanto mais rápido você pedir ajuda, maiores as chances de se recuperar de um prejuízo e de prevenir mais problemas.

OLHA A DICA:

Entre em contato com o suporte do seu serviço, ou aproveite as redes sociais para acompanhar profissionais de proteção de dados e Segurança da Informação e pedir ajuda, quando necessário.

PASSO 3: SIGA AS RECOMENDAÇÕES DE SEGURANÇA E USE FERRAMENTAS SEGURAS

Recomendações de Segurança

Você pode encontrar recomendações simples e fáceis de colocar em prática no nosso Ebook de Recomendações Importantes de Segurança para o seu negócio. Aprenda a gerenciar as suas senhas, ativar as camadas extras de segurança nas suas contas para se proteger de invasões, cuidar do seu ambiente de trabalho e muito mais!

Ferramentas Seguras

Também no nosso Ebook de Recomendações Importantes de Segurança para o seu negócio, você encontrará uma lista das ferramentas mais recomendadas para cuidar da sua Segurança, de forma descomplicada e com exemplos. Use apenas ferramentas reconhecidas e confiáveis, com boas recomendações.

Complemente o seu conhecimento com os nossos ebooks

Aproveite para combinar o conhecimento espalhado pelos nossos Ebooks, de acordo com o tamanho da sua empresa, seu plano de negócio, seus desafios e necessidades. Estamos aqui para te ajudar e impulsionar o seu sucesso!

